

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/001076

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2001-136159 A (Sony Corp.), 18 May, 2001 (18.05.01), Full text; Figs. 1 to 6	1-6, 10-12, 15, 16 14, 18
Y	Full text; Figs. 1 to 6 & WO 01/33771 A & EP 1143659 A	
X	JP 10-107832 A (Hitachi Software Engineering Co., Ltd.), 24 April, 1998 (24.04.98), Par. Nos. [0026] to [0028], [0044] to [0058]; Figs. 1 to 4	7-9, 13, 17 14, 18
Y	Par. Nos. [0026] to [0028], [0044] to [0058]; Figs. 1 to 4 (Family: none)	

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
27 April, 2004 (27.04.04)

Date of mailing of the international search report
18 May, 2004 (18.05.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/001076

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Claims 1-6, 10-12, 15, 16 relate to a broadcast key transmission for encrypting the payload or broadcast encryption key and the terminal identifier by the broadcast encryption key and transmitting them to another terminal.

Claims 7-9, 13, 17 relates to a unicast key distribution for encrypting and decrypting the broadcast key and the terminal identifier by the unicast encryption key.

(Continued to extra sheet)

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- ☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/001076

Continuation of Box No.III of continuation of first sheet(2)

Claims 14, 18 relate to a key distribution via a re-encryption processing for decrypting the broadcast encryption key and the terminal identifier which have been encrypted by the first terminal using the unicast encryption key, re-encrypting them by using the broadcast encryption key, and transmitting them to a third terminal.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. Cl⁷ H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1996年
日本国公開実用新案公報	1971-2004年
日本国登録実用新案公報	1994-2004年
日本国実用新案登録公報	1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X	J P 2001-136159 A (ソニー株式会社) 2001.05.18 全文, 図1-6	1-6, 10-12, 15, 16
Y	全文, 図1-6 & WO 01/33771 A & EP 1143659 A	14, 18

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」 特に関連のある文献ではなく、一般的技術水準を示すもの
「E」 国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」 優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
「O」 口頭による開示、使用、展示等に言及する文献
「P」 国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」 国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」 特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」 特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」 同一パテントファミリー文献

国際調査を完了した日

27.04.2004

国際調査報告の発送日

18.5.2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/J P)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

青木 重徳

5M

4229

電話番号 03-3581-1101 内線 3597

C (続き). 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
	JP 10-107832 A (日立ソフトウェアエンジニアリン グ株式会社)	
	1998. 04. 24	
X	第【0026】-【0028】段落,	7-9, 13, 17
	第【0044】-【0058】段落, 図1-4	
Y	第【0026】-【0028】段落,	14, 18
	第【0044】-【0058】段落, 図1-4	
	(ファミリーなし)	

第Ⅱ欄 請求の範囲の一部の調査ができないときの意見 (第1ページの2の続き)

法第8条第3項 (PCT 17条(2)(a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であってPCT規則6.4(a)の第2文及び第3文の規定に従って記載されていない。

第Ⅲ欄 発明の単一性が欠如しているときの意見 (第1ページの3の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲1-6, 10-12, 15, 16は、ペイロードあるいはブロードキャスト暗号鍵と端末識別子とをブロードキャスト暗号鍵で暗号化して他の端末に送信するブロードキャスト鍵配送に関するものである。

請求の範囲7-9, 13, 17は、ブロードキャスト鍵と端末識別子とをユニキャスト暗号鍵で暗号化、復号するユニキャスト鍵配送に関するものである。

請求の範囲14, 18は、第1の端末によりユニキャスト暗号鍵で暗号化されたブロードキャスト暗号鍵と端末識別子とを、第2の端末で復号しブロードキャスト暗号鍵により再暗号化して第3の端末に送信する再暗号処理を介した鍵配送に関するものである。

1. ☐ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☒ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☐ 追加調査手数料の納付と共に出願人から異議申立てがなかった。